

# Polynomial endomorphisms over finite fields: experimental results

Stefan Maubach    Roel Willems\*

Jacobs University	Radboud University Nijmegen
28759 Bremen	Postbus 9010, 6500 GL Nijmegen
Germany	The Netherlands
s.maubach@math.ru.nl	r.willems@math.ru.nl

January 15, 2013

## Abstract

Given a finite field  $\mathbb{F}_q$  and  $n \in \mathbb{N}^*$ , one could try to compute all polynomial endomorphisms  $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  up to a certain degree with a specific property. We consider the case  $n = 3$ . If the degree is low (like 2, 3, or 4) and the finite field is small ( $q \leq 7$ ) then some of the computations are still feasible. In this article we study the following properties of endomorphisms: being a bijection of  $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ , being a polynomial automorphism, being a *Mock automorphism*, and being a locally finite polynomial automorphism. In the resulting tables, we point out a few interesting objects, and pose some interesting conjectures which surfaced through our computations.

## 1 Introduction

**Notations and definitions:** Throughout this paper,  $\mathbb{F}_q$  will be a finite field of characteristic  $p$  where  $q = p^r$  for some  $r \in \mathbb{N}^*$ . When  $F_1, \dots, F_n \in k[X_1, \dots, X_n]$  ( $k$  a field), then  $F := (F_1, \dots, F_n)$  is a polynomial endomorphism over  $k$ . If there exists a polynomial endomorphism  $G$  such that  $F(G) = G(F) = (X_1, \dots, X_n)$ , then  $F$  is a polynomial automorphism (which is stronger than stating that  $F$  induces a

---

\*Funded by Phd-grant of council for the physical sciences, Netherlands Organisation for scientific research (NWO).

bijection on  $k^n$ ). We will write  $X$  for  $X_1, \dots, X_n$ . The polynomial automorphisms in  $n$  variables over  $k$  form a group, denoted  $\mathrm{GA}_n(k)$  (compare the notation  $\mathrm{GL}_n(k)$ ), while the set of polynomial endomorphisms is denoted by  $\mathrm{ME}_n(k)$  (the monoid of endomorphisms). If  $F \in \mathrm{GA}_n(k)$  such that  $\deg(F_i) = 1$  for all  $1 \leq i \leq n$ , then  $F$  is called affine. The affine automorphisms form a subgroup of  $\mathrm{GA}_n(k)$  denoted by  $\mathrm{Aff}_n(k)$ . In case  $F \in \mathrm{GA}_n(k)$  such that  $F_i \in k[X_i, \dots, X_n]$  for each  $1 \leq i \leq n$ , then  $F$  is called triangular, or Jonqui re. The triangular automorphisms form a subgroup of  $\mathrm{GA}_n(k)$ , denoted by  $\mathrm{J}_n(k)$ . The subgroup of  $\mathrm{GA}_n(k)$  generated by  $\mathrm{Aff}_n(k)$  and  $\mathrm{J}_n(k)$  is called the **tame automorphism group**, denoted by  $\mathrm{TA}_n(k)$ . By  $\deg(F)$  we will denote the maximum of  $\deg(F_i)$ . The set of polynomial maps of degree  $d$  or less we denote by  $\mathrm{ME}_n^d(k)$ , and the endomorphisms whose affine part is the identity we denote by  $\overline{\mathrm{ME}}_n(k)$ . The following notations are now natural:  $\overline{\mathrm{ME}}_n^d(k) := \overline{\mathrm{ME}}_n(k) \cap \mathrm{ME}_n^d(k)$ ,  $\mathrm{GA}_n^d(k) := \mathrm{ME}_n^d(k) \cap \mathrm{GA}_n(k)$ ,  $\overline{\mathrm{GA}}_n(k) := \overline{\mathrm{ME}}_n(k) \cap \mathrm{GA}_n(k)$ , and  $\overline{\mathrm{GA}}_n^d(k) := \overline{\mathrm{GA}}_n(k) \cap \mathrm{GA}_n^d(k)$ . If  $F, G \in \mathrm{ME}_n(k)$ , then  $F$  and  $G$  are called **equivalent (tamely equivalent)** if there exist  $N, M \in \mathrm{GA}_n(k)$  ( $N, M \in \mathrm{TA}_n(k)$ ) such that  $NFM = G$ . If  $F \in \mathrm{ME}_n(k)$  then we say that  $(F, X_{n+1}, \dots, X_{n+m}) \in \mathrm{ME}_{n+m}(k)$  is a stabilisation of  $F$ . We hence introduce the terms “**stably equivalent**” and “**stably tamely equivalent**” meaning that a stabilisation of  $F$  and  $G$  are equivalent or tamely equivalent.

The automorphism group  $\mathrm{GA}_n(k)$  is one of the basic objects in (affine) algebraic geometry, and the understanding of its structure a highly-sought after question. If  $n = 1$  then  $\mathrm{GA}_1(k) = \mathrm{Aff}_1(k)$ , and if  $n = 2$  then one has the Jung-van der Kulk theorem [4, 5], stating among others that  $\mathrm{GA}_2(k) = \mathrm{TA}_2(k)$ . However, in dimension 3 the structure of  $\mathrm{GA}_3(k)$  is completely dark. The only strong result is in fact a *negative* result by Umirbaev and Shestakov [9, 10], stating that if  $\mathrm{char} k = 0$ , then  $\mathrm{TA}_3(k) \neq \mathrm{GA}_3(k)$ .

It might be that all types of automorphisms known in  $\mathrm{GA}_3(k)$  have already surfaced, but the possibility exists that there are some strange automorphisms that have eluded common knowledge so far. But, in the case  $k = \mathbb{F}_q$ , we have an opportunity: one could simply check the finite set of endomorphisms up to a certain degree  $d$ , i.e.  $\mathrm{ME}_n^d(\mathbb{F}_q)$ , and determine which ones are automorphisms. Any “new” type of automorphisms *have* to surface in this way.

Unfortunately, the computations rapidly become unfeasible if the degree  $d$ , the number of variables  $n$ , or the size of the finite field  $\mathbb{F}_q$ , are too large. We didn’t find any significant shortcuts except the ones mentioned in section 2. In the end, for us scanning through lists of  $2^{30} = 8^{10}$  endomorphisms was feasible, but  $3^{20} = 9^{10}$  was barely out of reach.

In the case of  $k = \mathbb{F}_q$ , another interesting class that surfaces are the (what we define as) **mock automorphisms** of  $\mathbb{F}_q$ : endomorphisms which induce bijections of  $\mathbb{F}_q^n$ , and whose determinant of the Jacobian is a nonzero constant. Such maps are

interesting for example for cryptography (being “multivariate permutation polynomials”).

In this article, we do the (for us) feasible computations, and analyze the resulting lists. In particular, we compute (some of) the (mock) automorphisms for  $n = 3$ ,  $d \leq 3$ , and  $q \leq 5$ .

## 2 Generalities on polynomial automorphisms

The following lemma explains why we only study polynomial maps having affine part identity:

**Lemma 2.1.** *Let  $F \in \text{GA}_n^d(k)$ . Then there exists a unique  $\alpha, \beta \in \text{Aff}_n(k)$  and  $F', F'' \in \overline{\text{GA}}_n^d(k)$  such that*

$$F = \alpha F' = F'' \beta.$$

*Proof.* For the first equality, take  $\alpha$  to be the affine part of  $F$ , and define  $F' := \alpha^{-1}F$ . For the second, do the first equality for  $F^{-1}$ , i.e.  $F^{-1} = \gamma G$  for some  $\gamma \in \text{Aff}_n(k), G \in \overline{\text{GA}}_n(k)$ . Then  $F = G^{-1}\gamma^{-1}$  i.e. take  $\beta = \gamma^{-1}, F'' := G^{-1}$ . The fact that  $F'' \in \text{GA}_n^d(k)$  is easy to check by comparing the highest degrees of  $F''$  and  $F$ .  $\square$

A useful criterion is that if  $F$  is invertible, then  $\det(\text{Jac}(F)) \in k^*$ . The converse is a notorious problem in characteristic zero:

**Jacobian Conjecture:** (Short JC) If  $\text{char}(k) = 0$ ,  $F \in \text{ME}_n(k)$ , and  $\det(\text{Jac}(F)) \in k^*$ , then  $F$  is an automorphism.

The JC in  $\text{char}(k) = p$  is not true in general, as already in one variable,  $F(X_1) := X_1 - X_1^p$  has Jacobian  $1 - pX_1^{p-1} = 1$ , but  $F(0) = F(1)$  and so  $F$  is not a bijection. However, the following two (well-known) lemma's show that the Jacobian conjecture is true for the special case where  $\text{degree}(F) = 2$  and  $\text{char}(k) \geq 3$ .

**Lemma 2.2.** *Let  $F : k^n \rightarrow k^n$  be a polynomial endomorphism of degree 2 with  $\det(\text{Jac}(F))$  nowhere zero. Assume that  $\text{char}(k) = p \neq 2$ , then  $F$  is injective. In particular, if  $k$  is a finite field, then  $F$  is bijective.*

*Proof.* Suppose  $F$  is not injective, then there exist  $a, b \in k^n$  such that  $F(a) = F(b)$ . We may assume that  $a = 0 = F(a)$ , as we may replace  $F$  by  $F(a - X) - F(a)$  if necessary. Now consider  $F(tX) = F_0 + tF_1(X) + t^2F_2(X)$ , where  $F_i(X)$  is the homogeneous part of  $F(X)$  of degree  $i$  and  $t$  is a new variable. Then on the one hand  $\frac{d}{dt}F(tX) = F_1(X) + 2tF_2(X)$ , on the other hand  $\frac{d}{dt}F(tX) = \text{Jac}(F)|_{tX}X$ . Now if we substitute  $t = \frac{1}{2}$ , then on the one hand we get  $\frac{d}{dt}F(tX)|_{t=\frac{1}{2}} = F_1(X) + F_2(X) = F(X)$ , (by assumption  $F(0) = 0$ , so  $F_0 = 0$ ). And on the other hand we

get  $\frac{d}{dt}F(tX)|_{t=\frac{1}{2}} = \text{Jac}(F)|_{\frac{1}{2}X}X$ . But this means that  $0 = F(a) = \text{Jac}(F)|_{\frac{1}{2}a}a$  but since  $\det(\text{Jac}(F)|_{\frac{1}{2}a}) \neq 0$  it follows that  $\text{Jac}(F)|_{\frac{1}{2}a}$  is invertible, and this implies that  $a = 0$ , which contradicts our assumption that  $a \neq 0$ . So  $F$  is injective. If  $k$  is a finite field then  $k^n$  is a finite set, so injective implies bijective.  $\square$

**Corollary 2.3.** *Let  $F : k^n \rightarrow k^n$  be a polynomial endomorphism of degree 2 with  $\det(\text{Jac}(F)) = 1$ . Assume that  $\text{char}(k) \neq 2$ , then  $F$  is an automorphism.*

*Proof.* Let  $K$  be the algebraic closure of  $k$ . And consider  $F$  as a polynomial endomorphism of  $K^n$ . For every finite extension  $L$  of  $k$ , we have  $F : L^n \rightarrow L^n$  is a bijection, by the above lemma. Hence,  $F : K^n \rightarrow K^n$  is a bijection (as  $K$  is the infinite union of all finite extensions of  $k$ ). But  $K$  is algebraically closed so a bijection of  $K^n$  is a polynomial automorphism, so it has an inverse  $F^{-1}$ . Now Lemma 1.1.8 in [1] states that  $F^{-1}$  has coefficients in  $k$ , which means that  $F^{-1}$  is defined over  $k$ , which means that  $F$  is a polynomial automorphism over  $k$ .  $\square$

One remark on the previous result about the difference between  $\det(\text{Jac}(F)) = 1$  and  $\det(\text{Jac}(F))$  is nowhere zero. If  $\det(\text{Jac}(F))$  is nowhere zero over  $k$  this does not imply that  $\det(\text{Jac}(F))$  over  $K$  is nowhere zero, consider the following example (see the warning after Corollary 1.1.35 in [1]):

**Example 2.4.** Let  $F = (x, y + axz, z + bxy) \in k[x, y, z]$  with  $k$  a finite field of characteristic  $p$  and  $a, b \neq 0 \in k$ , such that  $ab$  is not a square. Then  $\det(\text{Jac}(F)) = 1 - abx^2$  is nowhere zero, but obviously  $F$  not invertible.

The following result is on subsets of groups that are invariant under a subgroup.

**Lemma 2.5.** *Let  $G$  be a group,  $H$  a finite subgroup of  $G$  and  $V$  a finite subset of  $G$  such that  $HV \subseteq V$ , then  $\#H | \#V$ .*

*Proof.* Since  $G$  acts transitively on  $G$ ,  $H$  acts transitively on  $V$ . Thus, for every  $v \in V$ ,  $Hv$  is an orbit set-isomorphic to  $H$ . Also,  $HV = V$  consists of disjoint orbits of the form  $Hv$ , so  $\#H | \#V$ .  $\square$

In this article we also consider so-called *locally finite polynomial automorphisms*. A motivation for studying these automorphisms is that they might generate the automorphism group in a natural way (see [3] for a more elaborate motivation of studying these maps). The reason that we make computations and classifications on them in this article is to have some examples on hand to work with in the future, as there can be rather complicated locally finite polynomial automorphisms.

**Definition 2.6.** *Let  $F \in \text{ME}_n(k)$ . Then  $F$  is called locally finite (short LFPE) if  $\deg(F^n)$  is bounded, or equivalently, there exists  $n \in \mathbb{N}$  and  $a_i \in k$  such that  $F^n + a_{n-1}F^{n-1} + \dots + a_1F + a_0I = 0$ . We say that  $T^n + a_{n-1}T^{n-1} + \dots + a_1T + a_0$*

is a vanishing polynomial for  $F$ . In [3] theorem 1.1 it is proven that these vanishing polynomials form an ideal of  $k[T]$ , and that there exists a minimum polynomial  $m_F(T)$ .

When trying to classify LFPEs and their minimal polynomials (i.e using computer calculations) one can use the following lemmas to reduce computations:

**Lemma 2.7.** *Let  $F \in \text{GA}_n(k)$  and  $L \in \text{GL}_n(k)$  then  $F$  is locally finite iff  $L^{-1}FL$  is locally finite. Furthermore if  $m(T) \in k[T]$  is the minimum polynomial for  $F$ , then  $m(T)$  is also the minimum polynomial of  $L^{-1}FL$ .*

*Proof.* Suppose  $F$  is locally finite with minimum polynomial  $m(T) = m_0 + m_1T + \dots + m_dT^d$ , so  $m_0I + m_1F + m_2F^2 + \dots + m_dF^d = 0$ , where  $I$  is the identity map, and  $F^d$  is the composition of  $d$   $F$ 's. Now  $0 = L^{-1}(m_0I + m_1F + m_2F^2 + \dots + m_dF^d)L = m_0L^{-1}IL + m_1L^{-1}FL + m_2L^{-1}F^2L + \dots + m_dL^{-1}F^dL = m_0I + m_1L^{-1}FL + m_2(L^{-1}FL)^2 + \dots + m_d(L^{-1}FL)^d = m(L^{-1}FL)$ . This shows that if  $F$  is locally finite with minimum polynomial  $m(T)$ , then so is  $L^{-1}FL$ .  $\square$

When classifying LFPEs, one cannot simply restrict to  $\overline{\text{GA}}_n(k)$ , as it is very well possible that  $F \in \overline{\text{GA}}_n(k)$  is not an LFPE, but  $\alpha F$  is where  $\alpha \in \text{Aff}_n(k)$ . However, we can restrict to classes of affine parts under linear maps, by the following lemma:

**Lemma 2.8.** *Let  $\alpha \in \text{Aff}_n(k)$  and  $F \in \overline{\text{GA}}_n^d(k)$ . Suppose that  $\beta = L^{-1}\alpha L$ , where  $L \in \text{GL}_n(k)$ , and that  $\beta F$  is locally finite. Now there exists an automorphism  $G \in \overline{\text{GA}}_n^d(k)$ , such that  $\beta F = L^{-1}\alpha GL$ , i.e.  $\beta F$  is in the conjugacy class of  $\alpha G$ . Furthermore, the minimum polynomials of  $F$  and  $G$  are the same.*

*Proof.* Just take  $G = LFL^{-1}$ , then  $L^{-1}\alpha GL = L^{-1}\alpha LFL^{-1}L = L^{-1}\alpha LF = \beta F$ .  $\square$

So in order to classify the locally finite automorphisms (up to some degree  $d$ ), it suffices to compute the conjugacy classes of  $\text{Aff}_n(k)$  under conjugacy by  $\text{GL}_n(k)$ , and compose a representative of each class with all the elements of  $\text{GA}_n^d(k)$ .

When considering LFPEs over finite fields, we have the additional following lemma:

**Lemma 2.9.** *Let  $F \in \text{GA}_n(\mathbb{F}_q)$  be an LFPE. Then  $F$  has finite order (as element of  $\text{GA}_n(\mathbb{F}_q)$ ).*

*Proof.* If  $F$  is an LFPE, then there exists a minimum polynomial  $m(T)$  generating the ideal of vanishing polynomials for  $F$ . There exists some  $r \in \mathbb{N}$  such that  $m(T) \mid T^{q^r} - T$ , yielding the result.  $\square$

Another concept that surfaces, is the following:

**Definition 2.10.** Let  $F = I + H \in \overline{\text{ME}}_n(k)$  where  $H = (H_1, \dots, H_n)$  is the non-linear part. Then  $F$  is said to satisfy the dependence criterion if  $(H_1, \dots, H_n)$  are linearly dependent.

Notice that  $F \in \overline{\text{ME}}_n(k)$  satisfying the dependence criterion is equivalent to being able to apply a linear conjugation to isolate one variable, i.e.  $L^{-1}FL = (X_1, X_2 + H_2, \dots, X_n + H_n)$  for some linear map  $L$ .

### 3 Computations on endomorphisms of low degree

It is clear that  $\#\text{Aff}_n(k) \mid \#\text{GA}_n^d(k)$ . Let  $F : k^n \rightarrow k^n$  be an automorphism then we can consider  $\alpha$  to be the affine part of  $F$ , which is obviously invertible and we can then look at  $G = \alpha^{-1}F$ , where  $G$  now has affine part the identity. This means that to compute all automorphisms it suffices to compute all automorphisms having affine part the identity and compose each of them from the left with all affine automorphisms. This suffices for our computations over  $\mathbb{F}_2$  and  $\mathbb{F}_3$ , but for larger finite fields ( $\mathbb{F}_4, \mathbb{F}_5$  and  $\mathbb{F}_7$ ) we will add additionally the dependence criterion.

Finally recall that over  $\mathbb{F}_q$  there are  $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$  linear automorphisms, and that there are  $q^n$  times as many affine automorphisms as linear.

For the rest of the article, as we stay in 3 dimensions, we will rename our variables  $x, y, z$ .

#### 3.1 The finite field of two elements: $\mathbb{F}_2$

As mentioned in the previous section to find all polynomial automorphisms it suffices to find all automorphisms having affine part equal to the identity, and there are  $(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$  linear automorphisms. There are  $2^3 * 168 = 1344$  affine automorphisms.

##### 3.1.1 Degree 2 over $\mathbb{F}_2$

We remind the reader that by a *mock automorphism* we mean an endomorphism  $E \in \text{ME}_n(k)$  such that  $E$  induces a permutation of  $k^n$  and  $\det(\text{Jac}(E)) \in k^*$ . Over  $\mathbb{F}_2$ , Corollary 2.3 does not hold so there do exist mock automorphisms which are not automorphisms in  $\text{ME}_3^2(\mathbb{F}_2)$ .

**Theorem 3.1.** If  $F \in \text{ME}_3^2(\mathbb{F}_2)$  is a mock automorphism, then  $F$  is in one of the following four classes:

- 1) The 176 tame automorphisms, equivalent to  $(x, y, z)$ .
- 2) 48 endomorphisms tamely equivalent to  $(x^4 + x^2 + x, y, z)$ .

3) 56 endomorphisms tamely equivalent to  $(x^8 + x^2 + x, y, z)$ .

4) 56 endomorphisms tamely equivalent to  $(x^8 + x^4 + x, y, z)$ .

In particular, all automorphisms of this type are tame, i.e.  $\text{GA}_3^2(\mathbb{F}_2) = \text{TA}_3^2(\mathbb{F}_2)$ . Furthermore, the equivalence classes are all distinct, except possibly class (3) and (4) (see conjecture 3.3).

There are in total  $1344 \cdot 176 = 236544$  automorphisms of  $\mathbb{F}_2^3$  of degree less or equal to 2.

*Proof.* The classification is done by computer, see [11] chapter 5. We can show how for example  $(x^8 + x^4 + x, y, z)$  is tamely equivalent to a polynomial endomorphism of degree 2:

$$\begin{aligned} (x + y^2, y + z^2, z)(x^8 + x^4 + x, y, z)(x, y + x^4 + x^2, z + x^2) = \\ (x + y^2, y + x^2 + z^2, z + x^2) \end{aligned}$$

What is left is to show that the classes (1),(2), and (3)+(4) are different. Class (1) consists of automorphisms while (2),(3),(4) are not. Using the below lemma 3.2, the endomorphisms of type (2) are all bijections of  $\mathbb{F}_{2^m}^3$  if  $3 \nmid m$ , and the endomorphisms of type (3) and (4) are all bijections of  $\mathbb{F}_{2^m}^3$  if  $7 \nmid m$ . The last sentence follows since  $\# \text{Aff}_3(\mathbb{F}_2) = 1344$ .  $\square$

**Lemma 3.2.**  $x^4 + x^2 + x$  is a bijection of  $\mathbb{F}_{2^r}$  if  $3 \nmid r$ , and  $x^8 + x^4 + x$  and  $x^8 + x^2 + x$  are bijection of  $\mathbb{F}_{2^r}$  if  $7 \nmid r$ .

*Proof.* Let us do  $f(x) := x^8 + x^4 + x$ , the other proofs go similarly.  $f$  is a bijection if and only if  $f$  is injective if and only if  $f(x) = f(y)$  has only  $x = y$  as solutions.  $f(x) = f(y)$  if and only if  $(x - y)^8 + (x - y)^4 + (x - y) = 0$ .  $x = y$  is a solution, another solution would be equivalent to finding a zero of  $x^7 + x^3 + 1$ . Now it is an elementary exercise to see that if  $\alpha \in \mathbb{F}_{2^r}$  is a zero of this polynomial, then  $7|r$ .  $\square$

**Question 3.3.** (1) Are  $F = (x^8 + x^2 + x, y, z)$  and  $G = (x^8 + x^4 + x, y, z)$  (tamely) equivalent?

(2) More general: Are  $x^8 + x^2 + x$  and  $x^8 + x^4 + x$  stably (tamely) equivalent?

The above question is particular to characteristic  $p$ , for consider the following:

**Lemma 3.4.** Let  $P, Q \in k[x]$ . Assume that  $F := (P(x), y, z)$  is equivalent to  $G := (Q(x), y, z)$ . Then  $P'$  and  $Q'$  are equivalent, in particular  $Q'(ax + b) = cP'$  for some  $a, b, c \in k$ ,  $ac \neq 0$ .

*Proof.* Equivalent means there exist  $S, T \in \text{GA}_3(k)$  such that  $SF = GT$ . Write  $J$  for  $\det(\text{Jac})$ . Now  $J(S) = \lambda, J(T) = \mu$  for some  $\lambda, \mu \in k^*$ . Using the chain rule we have

$$\begin{aligned} J(SF) &= J(F) \cdot (J(S) \circ (F)) = \frac{\partial P}{\partial x} \cdot (\lambda \circ (F)) = \lambda \frac{\partial P}{\partial x} \\ &= J(GT) = J(T) \cdot (J(G) \circ (T)) = \mu \cdot \left( \frac{\partial Q}{\partial x} \circ T \right) \end{aligned}$$

so

$$Q'(T) = \frac{\lambda}{\mu} P'$$

which means that  $T = (T_1, T_2, T_3)$  and  $T_1 = ax + b$  where  $a \in k^*, b \in k$ , proving the lemma.  $\square$

**Corollary 3.5.** *Assume  $\text{char}(k) = 0$ . Let  $P, Q \in k[x]$ . Assume that  $F := (P(x), y, z)$  is equivalent to  $G := (Q(x), y, z)$ . Then  $P$  and  $Q$  are equivalent.*

*Proof.* Lemma 3.4 shows that  $P'(ax + b) = cQ'$  for some  $a, b, c \in k, ac \neq 0$ . In characteristic zero we can now integrate both sides and get  $a^{-1}P(ax + b) = cQ$  proving the corollary.  $\square$

Note that in the “integrate both sides” part the characteristic zero is used, as  $(x + x^2 + x^8)' = (x + x^4 + x^8)'$  in characteristic 2.

Note that all the above one-variable polynomials  $x^8 + x^2 + x, x^4 + x^2 + x$  have a stabilisation which is tamely equivalent to a polynomial endomorphism of degree 2. In this respect, note the following proposition, which is lemma 6.2.5 from [1]:

**Proposition 3.6.** *Let  $F \in \text{ME}_n(k)$  where  $k$  is a field. Then there exists  $m \in \mathbb{N}$ , and  $G, H \in \text{TA}_{n+m}(k)$  such that (writing the stabilisation of  $F$  as  $\tilde{F} \in \text{ME}_{n+m}(k)$ )  $G\tilde{F}H$  is of degree 3 or less.*

### 3.1.2 Locally finite in degree 2 over $\mathbb{F}_2$

We now want to classify the locally finite automorphisms among the 236544 automorphisms over  $\mathbb{F}_2$  of degree 2 (or less), and we want to determine the minimum polynomial of each. Using lemma 2.7, we may classify up to conjugation by a linear map. We found 262 locally finite classes under linear conjugation, with the following minimum polynomials:



Minimum polynomial	#	$t$
$F^5 + F^4 + F + I$	16	8
$F^4 + F^3 + F^2 + I$	8	7
$F^4 + F^3 + F + I$	26	6
$F^4 + I$	12	4
$F^4 + F^2 + F + I$	8	7
$F^3 + F^2 + F + I$	139	4
$F^3 + F^2 + I$	2	7
$F^3 + F + I$	2	7
$F^3 + I$	14	3
$F^2 + I$	34	2
$F + I$	1	1

In the above tabular,  $\#$  denotes the number of *conjugacy classes* (i.e. not elements) having this minimum polynomial, while  $t$  denotes the order of the automorphism (see lemma 2.9). Furthermore, observe that  $\#$  displayed is the number of conjugacy classes that satisfy this relation, not the total number of automorphisms.

### 3.1.3 Degree 3 over $\mathbb{F}_2$

We only considered the endomorphisms of the form  $F = I + H$ , where  $H$  is homogeneous of degree 3. (The automorphisms of degree 3 or less in general was just out of reach.) The below tabular describes the set of  $F \in \text{ME}_3^3(\mathbb{F}_2)$  having the following criteria:

- $F$  is a mock automorphism,
- $F = I + H$ ,  $H$  homogeneous of degree 3.

We found 1520 endomorphisms satisfying the above requirements. The tabular lists them in 20 classes up to conjugation by linear maps:

	Representant	Bijection over	#
<b>1.</b>	<b><math>(\mathbf{x}, \mathbf{y}, \mathbf{z})</math></b>		
1a.	$(x, y, z)$	all	1
1b.	$(x, y, z + x^2y + xy^2)$	all	7
1c.	$(x, y, z + x^3 + x^2y + y^3)$	all	14
1d.	$(x, y + x^3, z + x^3)$	all	21
1e.	$(x, y, z + x^3 + x^2y + xy^2)$	all	21
1f.	$(x, y, z + x^2y)$	all	42
1g.	$(x, y + x^3, z + xy^2)$	all	42
1h.	$(x, y + x^3, z + x^2y + xy^2)$	all	42
1i.	$(x, y + z^3, z + x^2y)$	all	42
1j.	$(x, y + x^3, z + x^2y + y^3)$	all	84
1k.	$(x, y + x^3, z + y^3)$	all	84
<b>2.</b>	<b><math>(\mathbf{x}, \mathbf{y}, \mathbf{z} + \mathbf{x}^3\mathbf{z}^4 + \mathbf{x}\mathbf{z}^2)</math></b>		
2	$(x, y + x^3 + xz^2, z + xy^2 + xz^2)$	$\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}, \mathbb{F}_{32}$	56
<b>3.</b>	<b><math>(\mathbf{x}, \mathbf{y}, \mathbf{z} + \mathbf{x}^3\mathbf{z}^2 + \mathbf{x}^3\mathbf{z}^4)</math></b>		
3a.	$(x, y + xz^2, z + x^2y + xy^2)$	$\mathbb{F}_2, \mathbb{F}_4$	84
3b.	$(x, y + xz^2, z + x^3 + x^2y + xy^2)$	$\mathbb{F}_2, \mathbb{F}_4$	84
<b>4.</b>	<b><math>(\mathbf{x}, \mathbf{y}, \mathbf{z} + \mathbf{x}\mathbf{z}^2 + \mathbf{x}\mathbf{z}^6)</math></b>		
4a.	$(x, y + x^3 + z^3, z + x^3 + xy^2 + xz^2)$	$\mathbb{F}_2$	168
4b.	$(x, y + z^3, z + xy^2 + xz^2)$	$\mathbb{F}_2$	168
<b>5.</b>	<b><math>(\mathbf{x}, \mathbf{y}, \mathbf{z} + \mathbf{x}^3\mathbf{z}^2 + \mathbf{x}\mathbf{y}^2\mathbf{z}^4 + \mathbf{x}^2\mathbf{y}\mathbf{z}^4 + \mathbf{x}^3\mathbf{z}^6)</math></b>		
5a.	$(x, y + xz^2, z + xy^2 + y^3)$	$\mathbb{F}_2$	168
5b.	$(x, y + xz^2, z + x^3 + x^2y + y^3)$	$\mathbb{F}_2$	168
<b>6.</b>	<b><math>(\mathbf{x}, \mathbf{y}, \mathbf{z} + \mathbf{x}^3\mathbf{z}^2 + \mathbf{x}\mathbf{y}^2\mathbf{z}^2 + \mathbf{x}^2\mathbf{y}\mathbf{z}^4 + \mathbf{x}^3\mathbf{z}^6)</math></b>		
6.	$(x, y + xy^2 + xz^2, z + x^3 + x^2y)$	$\mathbb{F}_2$	168
<b>7.</b>	<b><math>(\mathbf{x} + \mathbf{y}^2\mathbf{z}, \mathbf{y} + \mathbf{x}^2\mathbf{z} + \mathbf{y}^2\mathbf{z}, \mathbf{z} + \mathbf{x}^3 + \mathbf{x}\mathbf{y}^2 + \mathbf{y}^3)</math></b>		
7.	$(x + y^2z, y + x^2z + y^2z, z + x^3 + xy^2 + y^3)$	$\mathbb{F}_2$	56

The first column gives a representant up to linear conjugation, and the bold fonted one gives a representant under tamely equivalence for the classes listed beneath it. The second column lists for which field extensions (from  $\mathbb{F}_{2^r}$  where  $1 \leq r \leq 5$ ) the map is also a bijection of  $\mathbb{F}_{2^r}^3$ . Class 1 are the 400 automorphisms, all of them are tame and satisfy the dependence conjecture. All classes are tamely equivalent to a map of the form  $(x, y, P(x, y, z))$ , except the last class 7 - these maps do not satisfy the Dependence Criterium, which makes them very interesting!

The above tabular might make one think that any mock automorphism in  $\text{ME}_3(\mathbb{F}_2)$  of the form  $F = (x, y + H_2, z + H_3)$  where  $H_2, H_3$  are homogeneous of the same degree, then one can tamely change the map into one of the form  $(x, y, z + K)$ , but the below conjecture might give a counterexample:

**Conjecture 3.7.** *Let  $F = (x, y + y^8 z^2 + y^2 z^8, z + y^6 z^4 + y^4 z^6)$ . Then  $F$  is not tamely equivalent to a map of the form  $(x, y, z + K)$ .*

Due to our lack of knowledge of the automorphism group  $\mathrm{TA}_3(\mathbb{F}_2)$ , this conjecture is a hard one unless one finds a good invariant of maps of the form  $(x, y, z + K)$ .

## 3.2 The finite field of three elements: $\mathbb{F}_3$

### 3.2.1 Degree 2 over $\mathbb{F}_3$

Over  $\mathbb{F}_3$ , there are  $(27 - 1)(27 - 3)(27 - 9) = 11232$  linear automorphisms and  $27 * 11232 = 303264$  affine automorphisms.

From corollary 2.3 it follows that if  $\det(\mathrm{Jac}(F)) = 1$  and  $\deg(F) \leq 2$ , then  $F$  is an automorphism - so we will not encounter any mock automorphisms which aren't an automorphism in this class. There are 2835 automorphisms of degree less or equal to 2 having affine part identity, so there are  $2835 \cdot 303264 =$  automorphisms of degree 2 or less. They all turned out to be tame.

### 3.2.2 Locally finite

We computed all conjugacy classes under linear maps of locally finite automorphisms of  $\mathbb{F}_3^3$  (see lemma 2.8). There are 80 orbits of affine automorphisms, composing a representative of each class with all of the 2,835 tame automorphisms, gives us 226,800 representatives of "conjugacy classes". We checked for each of them whether it was locally finite or not. It turns out that 25,872 of these conjugacy classes are locally finite. And there are exactly a hundred different minimum polynomials that can appear.

Of the appearing minimal polynomials in this list, all polynomials of degree 3 appear in this list. The highest minimum polynomials are of degree 10. We list just a (sort of random, non-affine) ten minimum polynomials, their order (which is determined by the minimum polynomial), number of *conjugacy classes* with this minimum polynomial, and one example. The reader interested in the complete list we refer to chapter 6 of the Ph.-D. thesis of the second author [11].

Minimum polynomial	order	#	example
$F^2 + 2I$	2	509	$\begin{pmatrix} 2x^2 + xy + xz + 2x + y^2 + z^2 \\ 2x^2 + xy + xz + y^2 + 2y + z^2 \\ 2x^2 + xy + xz + y^2 + z^2 + 2z \end{pmatrix}$
$F^3 + F^2 + 2F + 2I$	6	5084	$\begin{pmatrix} x^2 + xy + 2x + y^2 \\ x^2 + xy + y^2 + 2y \\ 2x^2 + 2y^2 + 2z \end{pmatrix}$
$F^4 + 2F^2 + 2F + 2I$	24	2	$\begin{pmatrix} x^2 + xz + 2x + y^2 + 2y + z^2 \\ 2x + y + z \\ x^2 + xz + x + y^2 + y + z^2 + z \end{pmatrix}$
$F^4 + 2F^3 + 2F + I$	9	3804	$\begin{pmatrix} 2x^2 + 2xy + x + 2y^2 + 1 \\ 2x^2 + 2xy + 2y^2 + y + 1 \\ 2x^2 + xy + 2x + 2y^2 + z + 1 \end{pmatrix}$
$F^4 + F^3 + F^2 + 2F + I$	8	38	$\begin{pmatrix} x^2 + 2xy + xz + x + y^2 + yz + z^2 + 2z + 2 \\ x^2 + 2xy + xz + y^2 + yz + z^2 + 2z \\ 2x^2 + xy + 2xz + 2x + 2y^2 + 2yz + 2y + 2z^2 + 2 \end{pmatrix}$
$F^5 + 2F^3 + 2F^2 + F + 2I$	8	8	$\begin{pmatrix} 2x^2 + xy + xz + y^2 + 2y + z^2 \\ 2x^2 + xy + xz + 2x + y^2 + 2y + z^2 + z \\ 2x^2 + xy + xz + x + y^2 + z^2 + z \end{pmatrix}$
$F^6 + F^5 + 2F^4 + F^3 + 2I$	24	16	$\begin{pmatrix} y^2 + yz + 2y + z^2 \\ 2x + y^2 + yz + 2y + z^2 + z \\ x + y^2 + yz + z^2 + z \end{pmatrix}$
$F^7 + F^6 + 2F + 2I$	18	396	$\begin{pmatrix} 2x^2 + 2xz + 2y^2 + 2y + 2z^2 + 2z + 1 \\ x^2 + xz + 2y + z^2 \\ 2x^2 + 2xz + 2x + 2y^2 + 2y + 2z^2 + 2 \end{pmatrix}$
$F^{10} + F^8 + 2F^5 + F^2 + 2F + 2I$	26	40	$\begin{pmatrix} y + 2z^2 + z + 1 \\ x^2 + 2xz + x + z^2 + 1 \\ x + z + 1 \end{pmatrix}$
$F^{10} + F^9 + 2F^8 + F^7 + F^6 + F^5 + 2F^3 + 2F + I$	13	48	$\begin{pmatrix} 2x^2 + 2xy + 2xz + y^2 + yz + y + 2z^2 + 2z + 1 \\ 2x + y + z + 2 \\ 2x^2 + 2xy + 2xz + 2x + yz + y + 2z^2 + 2z + 1 \end{pmatrix}$

### 3.2.3 Degree 3 over $\mathbb{F}_3$

The amount of elements in  $\overline{\text{ME}}_3(\mathbb{F}_3)$  of the form  $(x, y, z) + (0, H_2, H_3)$  (i.e. satisfying the dependency criterion) where  $H_2, H_3$  are homogeneous of degree 3 is too large: this set has  $3^{20}$  elements which was too large for our system to scan through; however, we think that this case is feasible for someone having a stronger, dedicated system and a little more time.

## 3.3 The finite fields $\mathbb{F}_4$ and $\mathbb{F}_5$

In this section we will only restrict to degree 2, and to the maps which satisfy the dependency conjecture. Thus, in this section we restrict to maps  $F$  of the form  $(x + H_1, y + H_2, z)$  where  $H_1, H_2$  are of degree 2.

## 3.4 The finite field $\mathbb{F}_4$

There are  $(64-1)(64-4)(64-16) = 181,440$  linear automorphisms and  $64 \cdot 181,440 = 11,612,160$  affine automorphisms. We considered the following maps:

- $F \in \overline{\text{ME}}_3^2(\mathbb{F}_4)$ ,
- $F$  is a mock automorphism,
- $F$  is of the form  $(x + H_1(x, y, z), y + H_2(x, y, z), z)$  (i.e.  $F$  satisfies the dependency criterion).

and we counted 40,384 such maps. Under tame equivalence, we have the following classes:

- 1  $(x, y, z)$  (tame automorphisms)
- 2  $(x + x^2 + x^4, y, z)$

So, surprisingly, we only find a subset of the classes we found over  $\mathbb{F}_2$ . Well, not really surprising - the dependency criterion removes the classes 3 and 4 of theorem 3.1 from the list. We conjecture that the four classes of theorem 3.1 are the same for  $\mathbb{F}_4$ :

**Conjecture 3.8.** (i) Suppose  $F \in \text{ME}_3^2(\mathbb{F}_4)$  is a mock automorphism of  $\mathbb{F}_4$ . Then  $F$  is tamely equivalent to  $(P(x), y, z)$  where

$$P = x, P = x^4 + x^2 + x, P = x^8 + x^4 + x, \text{ or } P = x^8 + x^2 + x.$$

(ii) Suppose  $F \in \text{ME}_3^2(L)$  is a mock automorphism of  $L$ , where  $[L : \mathbb{F}_2] < \infty$ . Then  $F$  is tamely equivalent to  $(P(x), y, z)$  where

$$P = x, P = x^4 + x^2 + x, P = x^8 + x^4 + x, \text{ or } P = x^8 + x^2 + x.$$

If  $3 \mid [L : \mathbb{F}_2]$  then one should remove the class of  $P = x^4 + x^2 + x$ , and if  $7 \mid [L : \mathbb{F}_2]$  then one should remove the classes of  $P = x^8 + x^4 + x$  and  $P = x^8 + x^2 + x$ .

It would be interesting to see a proof of this conjecture by theoretical means - or a counterexample of course.

### 3.5 The finite field $\mathbb{F}_5$

There are  $(125 - 1)(125 - 5)(125 - 25) = 1,488,000$  linear automorphisms and  $125 \cdot 1,488,000 = 1,86,000,000$  affine automorphisms. We consider maps of the following form: There are 3,625 mock automorphisms of  $\mathbb{F}_5$  of degree at most 2. endomorphisms satisfying the following:

- $F \in \overline{\text{ME}}_3^2(\mathbb{F}_5)$ ,
- $F$  is a mock automorphism of  $\mathbb{F}_5$ ,
- $F$  satisfies the dependency criterion (i.e.  $F = (x + H_1(x, y, z), y + H_2(x, y, z), z)$ ).

We counted 3,625 such maps - and because of Corollary 2.3, they are all automorphisms. They all turned out to be tame maps.

## 4 Conclusions

We can gather some of the results in the below theorem:

**Theorem 4.1.** *Let  $F \in \text{GA}_3^d(\mathbb{F}_q)$ . If one of the below conditions is met, then  $F$  is tame:*

- $d = 3, q = 2,$
- $d = 2, q = 3,$
- $d = 2, q = 4$  or  $5,$  and  $F$  satisfies the Dependency criterion.

This gives rise to the following conjecture:

**Conjecture 4.2.** *If  $F = I + H \in \text{GA}_n(k)$  where  $H$  is homogeneous of degree 2, then  $F$  is tame.*

This natural conjecture might have been posed before, but we are unaware. This article proves this conjecture for  $n = 3$  and  $k = \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$ . We expect that for  $n = 3$  and a generic field a solution is within reach.

Unfortunately, the computations did not allow us to go as far as finding some candidate non-tame automorphisms (though the Nagata automorphism is one, however it is of too high degree). However, one of the interesting conclusions is that the set of *classes* (under tame automorphisms) of mock automorphisms seems to be much smaller than we originally expected: only 4 (perhaps 3) over  $\mathbb{F}_2$  up to degree 2, and at most 7 over  $\mathbb{F}_2$  of degree 3. In particular, we are puzzled by the interesting question whether the two endomorphisms over  $\mathbb{F}_2$  described by  $(x^8 + x^4 + x, y)$  and  $(x^8 + x^2 + x, y)$  are not equivalent, as stated in question 3.3.

**Computations:** For computations we used the MAGMA computer algebra program. The reader interested in the routines we refer to chapter 6 of the thesis of the second author, [11]. Also, we possess databases usable in MAGMA, which we hope to share in the near future on a website.

**Acknowledgements:** The second author would like to thank Joost Berson for some useful discussions.

## References

- [1] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, volume 190 of *Progress in Mathematics*, Birkhäuser (2000)

- [2] A. van den Essen, H. Huy Vui, H. Kraft, P. Russell and D. Wright, *Polynomial automorphisms and related topics*, Lecture notes of the international school and workshop ICPA2006, october 2006, Institute of Mathematics, Hanoi, Vietnam.
- [3] J-Ph. Furter, S. Maubach, *Locally finite polynomial endomorphisms*, J. Pure Appl. Algebra 211 (2007), no. 2, 445-458
- [4] H.W.E. Jung, *Über ganze birationale Transformationen der Ebene*, (German) J. Reine Angew. Math. 184, (1942). 161-174.
- [5] W. van der Kulk, *On polynomial rings in two variables*, Nieuw Arch. Wiskunde (3) 1, (1953). 33-41.
- [6] S. Maubach, *The automorphism group over finite fields*, Serdica Math. J. 27 (2001) n0.4. 343-350.
- [7] S. Maubach, *A problem on polynomial maps over finite fields*, unpublished preprint (2008), arXiv:0802.0630
- [8] S. Maubach and R. Willems, *Polynomial automorphisms over finite fields: Mimicking non-tame and tame maps by the Derksen group*, preprint (2010).
- [9] I. Shestakov, U.Umirbaev, *The tame and the wild automorphisms of polynomial rings in three variables*, J. Amer. Math. Soc. 17 (2004), no. 1, 197-227
- [10] I. Shestakov, U.Umirbaev, *Poisson brackets and two-generated subalgebras of rings of polynomials*, J. Amer. Math. Soc. 17 (2004), no. 1, 181-196
- [11] R. Willems, *Polynomial automorphisms and Mathieu subspaces*, Ph.-D. thesis, Radboud University, to appear (2011).